UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/799,455	03/12/2004	Sean E. Purcell	MS308121.1/MSFTP644US	7697

27195   7590   06/15/2009
TUROCY & WATSON, LLP
127 Public Square
57th Floor, Key Tower
CLEVELAND, OH 44114

EXAMINER
MAI, KEVIN S

ART UNIT	PAPER NUMBER
2456	

NOTIFICATION DATE	DELIVERY MODE
06/15/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docket1@thepatentattorneys.com
hholmes@thepatentattorneys.com
lpasterchek@thepatentattorneys.com

<table>
<tr><td rowspan="2">Office Action Summary</td><td>Application No.
10/799,455</td><td>Applicant(s)
PURCELL ET AL.</td></tr>
<tr><td>Examiner
KEVIN S. MAI</td><td>Art Unit
2456</td></tr>
</table>

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 February 2009*.
2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9-13,15-20,22,24,25,27,29,30 and 34* is/are pending in the application.
  4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) *1-7,9-13,15-20,22,24,25,27,29,30 and 34* is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
  Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
  Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  a)☐ All   b)☐ Some * c)☐ None of:
    1.☐ Certified copies of the priority documents have been received.
    2.☐ Certified copies of the priority documents have been received in Application No. _____.
    3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
  * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☒ Information Disclosure Statement(s) (PTO/SB/08)
  Paper No(s)/Mail Date *3/3/09*.
4)☐ Interview Summary (PTO-413)
  Paper No(s)/Mail Date. _____ .
5)☐ Notice of Informal Patent Application
6)☐ Other: _____ .

DETAILED ACTION

1.   This Office Action has been issued in response to Applicant's Amendment filed February 27, 2009.

2.   Claims 1-5, 9-13, 16, 22, 27, 29 and 34 have been amended. Claims 8, 14, 21, 23, 26, 28, 31-33 and 35-44 have been canceled. Claims 1-7, 9-13, 15-20, 22, 24, 25, 27, 29, 30 and 34 have been examined and are pending.

Response to Arguments

3.   Applicant's arguments filed February 27, 2009 have been fully considered but they are not persuasive.

4.   Applicant's arguments with respect to claim 1 have been considered but they are not persuasive. Applicant argues that Rajan, Daniell and Wendkos fail to disclose "a filtering component that identifies whether content of at least one message comprises text, one or more images, one or more sounds, one or more videos, one or more URLs, embedded content, one or more attachments, or one or more applets offensive to the user" and " a content blocking component that partially blocks the content of the at least one message by preventing offensive portions thereof from being viewed or sensed from at least a preview pane that displays the at least one message". Examiner disagrees. The current claim 1 rejection has been changed to be under Daniell alone or Daniell in view of Wendkos, however examiner will still address the arguments since they would still apply to the current references.

5.   With respect to the "filtering component that identifies whether content of at least one message comprises text ... offensive to the user", Daniell discloses this (Figure 4 of Daniell

discloses a text filtering component that can be used to scan incoming mail for offensive words

and phrases).

6.   Then with respect to "a content blocking component that partially blocks the content",

Daniell somewhat discloses this, figure 9B of Daniell discloses allowing a user to make

substitutions of objectionable words or phrases. This is seen to be disclosing partially blocking

content by preventing offensive portions of the message from being viewed. While this is being

done manually by a parent for a child it nonetheless discloses the email client containing a

feature used to detect objectionable words for the purpose of replacing them with acceptable

words to prevent only the objectionable content from being viewed. However, additionally,

Daniell in view of Wendkos also discloses the limitation, paragraph [0008] of Wendkos discloses

striping out all images and links from incoming email in an attempt to thwarts computer users

from being exposed to offensive images and dangerous links. As seen Wendkos only partially

blocks the content of the emails, namely the images and links. However, applicant argues that

because Wendkos merely discloses all images and links being indiscriminately removed it does

not read upon the claimed limitation. While examiner cannot dispute that Wendkos discloses

removing all images, the rejection was made with Daniell in view of Wendkos. Wherein Daniell

discloses filtering contents to identify offensive content and Wendkos was brought in to disclose

the idea of partially removing content from messages. Thus it is their combination that teaches

the disclosed limitation.

7.   Applicant's arguments with respect to claim 2 have been considered but they are not

persuasive. Applicant argues that Rajan, Daniell, and Wendkos fail to disclose calculating a junk

score for the at least one message. Examiner disagrees. Rajan discloses that each piece of

incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in

paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded

along a 0 - 100 range and this is seen to be a junk score for the messages.

8.   Applicant further argues that the references fail to disclose a classification component

that classifies the at least one message as any one of a good state, a junk state, and a middle state

based in part on the junk score. Examiner disagrees. Paragraph [0016] of Rajan discloses an

example of a spam scale from 0 - 100 where messages that scored above 80 would be labeled

"black", messages scoring between 30 - 80 would be labeled "gray" and then messages below 30

would be left in the inbox. This is seen to be the same as having a good, junk, and middle state

9.   Applicant further argues that the references fail to disclose the middle state indicates that

the at least one message is determined to be safe for an inbox, but not safe for viewing or

previewing in at least the preview pane without partial blocking of content of the at least one

message. Examiner disagrees. Paragraph [0032] of Rajan discloses that some email may be

placed in more than one directory such as the inbox (white) directory and the gray directory.

Then in paragraph [0043] of Daniell it is disclosed that the feature of displaying a preview of a

selected message can be disabled for spam messages. Thus it is seen that those that are rated

gray/white would be in the inbox but since it is spam would still have the have the content be

filtered as disclosed in Daniell.

10.   Applicant's arguments with respect to the remaining claims have been considered but

they are not persuasive. Applicant supplies the same arguments that are used for the claims

above and as such examiner recites the same response used above.

Claim Rejections - 35 USC § 101

11.   In view of the amendments/cancellations made to claims 1-20, 22-39 and 41-43 the

pending claim rejections under 35 USC § 101 have been withdrawn.

Claim Rejections - 35 USC § 112

12.   In view of the amendments/cancellations made to claims 1-44 the pending claim

rejections under 35 USC § 112 have been withdrawn.

Claim Rejections - 35 USC § 103

13.   The text of those sections of Title 35, U.S. Code not included in this action can be found

in a prior Office action.

14.   Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Pub. No.

2005/0097174 to Daniell et al. (hereinafter "Daniell").

15.   **As to Claim 1,** Daniell discloses **a system that mitigates viewing offensive message**

content comprising:

a processor that executes the following computer executable components stored on a

computer readable medium (Figure 1 and paragraph [0024] of Daniell disclose a processor)**;**

a message receiving component that receives at least one message for delivery to a user

(Figure 1 and paragraph [0024] of Daniell disclose the workstations containing an email

application that allows the work station to send and receive email messages through the

network);

a filtering component that <u>that identifies whether content of the at least one message</u>

<u>comprises text, one or more images, one or more sounds, one or more videos, one or more</u>

<u>URLs, embedded content, one or more attachments, or one or more applets offensive to the</u>

<u>user</u> (Figure 4 of Daniell discloses a text filtering component that can be used to scan incoming

mail for offensive words and phrases)**; and**

a content blocking component that blocks <u>the content of the at least one message by</u>

<u>preventing offensive portions thereof from being viewed or sensed from at least a preview</u>

<u>pane that displays the at least one message</u> (Paragraph [0043] of Daniell discloses that, for the

spam folder, the feature of displaying a preview of a selected message has been disabled. This is

because the message has been determined to be objectionable or undesired)**.**

Daniell does not explicitly disclose **partially** blocking content.

However, it would have been obvious in view of Daniell's disclosure. Figure 9B of

Daniell discloses allowing a user to make substitutions of objectionable words or phrases. This

is seen to be disclosing partially blocking content by preventing offensive portions of the

message from being viewed. While this is being done manually by a parent for a child it

nonetheless discloses the email client containing a feature used to detect objectionable words for

the purpose of replacing them with acceptable words to prevent only the objectionable content

from being viewed.

It would have been obvious to one of ordinary skill in the art at the time of invention to

combine preventing messages from being viewed in the preview pane as disclosed by Daniell,

with preventing only the objectionable content from being viewed as disclosed by Daniell. One

of ordinary skill in the art would have been motivated to combine to prevent unintentional

viewing of content determined to be objectionable or undesired. Since the purpose of a spam

filtering is to prevent the user from viewing content they do not wish to view, it would be

obvious to prevent the user from seeing the content via the preview pane because the content has

been determined to be objectionable or undesired (Paragraph [0043] of Daniell).

16.   Claims 1, 5, 6 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Daniell and further in view of US Pub. No. 2005/0228899 to Wendkos et al. (hereinafter

"Wendkos").

17.   **As to Claim 1,** Daniell discloses **a system that mitigates viewing offensive message

content comprising:**

a processor that executes the following computer executable components stored on a

computer readable medium (Figure 1 and paragraph [0024] of Daniell disclose a processor) **;**

a message receiving component that receives at least one message for delivery to a user

(Figure 1 and paragraph [0024] of Daniell disclose the workstations containing an email

application that allows the work station to send and receive email messages through the

network);

a filtering component that that identifies whether content of the at least one message

comprises text, one or more images, one or more sounds, one or more videos, one or more

URLs, embedded content, one or more attachments, or one or more applets offensive to the

user (Figure 4 of Daniell discloses a text filtering component that can be used to scan incoming mail for offensive words and phrases)**; and**

a content blocking component that blocks <u>the content of the at least one message by preventing offensive portions thereof from being viewed or sensed from at least a preview pane that displays the at least one message</u> (Paragraph [0043] of Daniell discloses that, for the spam folder, the feature of displaying a preview of a selected message has been disabled. This is because the message has been determined to be objectionable or undesired)**.**

Daniell does not explicitly disclose **partially** blocking content.

However, Wendkos discloses this (Paragraph [0008] of Wendkos discloses striping out all images and links from incoming email in an attempt to thwarts computer users from being exposed to offensive images and dangerous links. As seen Wendkos only partially blocks the content of the emails, namely the images and links)

It would have been obvious to one of ordinary skill in the art at the time of invention to combine disabling a preview pane as disclosed by Rajan-Daniell, with striping out images and links as disclosed by Wendkos. One of ordinary skill in the art would have been motivated to combine to thwart users from being exposed to offensive images and dangerous links (Paragraph [0008] of Wendkos).

18.   **As to Claim 5,** Daniell-Wendkos discloses **the system of claim 1, further comprising an unblocking component that receives user input to unblock the <u>partially</u> blocked <u>content</u> of the at least one message in at least the preview pane** (Paragraph [0044] of Daniell discloses that messages in the spam folder may be unmarked as spam and the message that has been stored

in the spam folder would be moved to the inbox folder of the user. Since the preview pane is

fully enabled in the inbox it is seen that the blocked portion of the message would now be

unblocked and viewable in the preview pane).

19.   **As to Claim 6,** Daniell-Wendkos-Rajan discloses **wherein the system of claim 5, the**

unblocking component operates per message (Paragraph [0044] of Daniell discloses that

messages in the spam folder may be unmarked as spam and the message that has been stored in

the spam folder would be moved to the inbox folder of the use. This only being applied to the

selected message and as such is operating per message).

20.   **As to Claim 10,** Daniell-Wendkos discloses **the system of claim 1, wherein the content**

blocking component partially blocks the content of the at least one message by performing

at least one of the following:

hiding the content of the at least one message in at least the preview pane (Paragraph [0043]

of Daniell discloses that, for the spam folder, the feature of displaying a preview of a selected

message has been disabled. This is because the message has been determined to be objectionable

or undesired. Then paragraph [0008] of Wendkos discloses stripping out all images and links

from incoming email. Thus it is seen that Wendkos discloses partially blocking using at least

one of the listed limitations);

hiding a portion of a subject line of the at least one message;

hiding a portion of content in a from line of the at least one message;

blurring a portion of the subject line of the at least one message;

blurring a portion of content in the from line of the at least one message; or

blurring a portion of the content of the at least one message in at least the preview pane.

21.   Claims 2-4, 7, 9, 18-20, 22, 24, 25, 27 and 34 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Daniell-Wendkos and further in view of U.S. Pub. No. 2005/0165895 to

Rajan et al. (hereinafter "Rajan").

22.   **As to Claim 2,** Daniell-Wendkos discloses **the system of claim 1, further comprising:**

        Daniell-Wendkos does not explicitly disclose **calculating a junk score for the at least**

one message; and

        However, Rajan discloses this (Paragraph [0015] of Rajan discloses that each piece of

incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in

paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded

along a 0 - 100 range and this is seen to be a junk score for the messages)

        It would have been obvious to one of ordinary skill in the art at the time of invention to

combine the system of claim 1 as disclosed by Daniell-Wendkos, with calculating a junk score as

disclosed by Rajan. One of ordinary skill in the art would have been motivated to combine

because both systems disclose spam filtering and as such substituting one systems spam finding

algorithm for the other would be obvious to one of ordinary skill in the art. It would be seen as

simple substitution of one known element for another. Wherein one of ordinary skill in the art

would be further motivated to combine to improve the situation where too many or too few

emails are classified as spam (Paragraphs [0009] and [0010] of Rajan)

Daniell-Wendkos does not explicitly disclose **a classification component that classifies the at least one message as any one of a good state, a junk state, and a middle state based in part on the junk score** (Paragraph [0016] of Rajan discloses an example of a spam scale from 0 - 100 where messages that scored above 80 would be labeled "black", messages scoring between 30 - 80 would be labeled "gray" and then messages below 30 would be left in the inbox. This is seen to be the same as having a good, junk, and middle state);

Examiner recites the same rationale to combine used above.

<u>wherein the middle state indicates that the at least one message is determined to be safe for an inbox, but not safe for viewing or previewing in at least the preview pane without partial blocking of content of the at least one message </u>(Paragraph [0032] of Rajan discloses that some email may be placed in more than one directory such as the inbox (white) directory and the gray directory. Then in paragraph [0043] of Daniell it is disclosed that the feature of displaying a preview of a selected message can be disabled for spam messages. Thus it is seen that those that are rated gray/white would be in the inbox but since it is spam would still have the have the content be filtered as disclosed in Daniell-Wendkos).

Examiner recites the same rationale to combine used above.

23.   **As to Claim 3,** Daniell-Wendkos-Rajan discloses **the system of claim 2, wherein the <u>at least one</u> message is classified at least in the middle state when the junk score exceeds at least the first threshold** (Paragraph [0016] of Rajan discloses an example of a spam scale from 0 - 100 where messages that scored above 80 would be labeled "black", messages scoring between 30 - 80 would be labeled "gray" and then messages below 30 would be left in the inbox.

Thus it is seen that exceeding the first threshold of 30 in this situation would be classifying a

message in the middle state).

Examiner recites the same rationale to combine used in claim 2.

24.   **As to Claim 4,** Daniell-Wendkos-Rajan discloses **the system of claim 2, further**

comprising an analysis component that determines whether the junk score exceeds a first

threshold (Paragraph [0016] of Rajan discloses an example of a spam scale from 0 - 100 where

messages that scored above 80 would be labeled "black", messages scoring between 30 - 80

would be labeled "gray" and then messages below 30 would be left in the inbox. This

classification step is seen to imply that determination of a message exceeding a threshold is done

by the system).

Examiner recites the same rationale to combine used in claim 2.

25.   **As to Claim 7,** Daniell-Wendkos-Rajan discloses **wherein the system of claim 1, the**

content blocking component operates per message or globally for substantially all messages

(Paragraph [0032] of Rajan discloses that some email may be placed in more than one directory

such as the inbox (white) directory and the gray directory. Then in paragraph [0043] of Daniell

it is disclosed that the feature of displaying a preview of a selected message can be disabled for

spam messages. Thus it is seen that those that are rated gray/white would be in the inbox but

since it is spam those messages would still have the preview disabled. This scenario represents

blocking operating per message. However in paragraph [0043] of Daniell the preview window

being disabled applies to the whole spam folder, this implies the ability to disable the preview

window for specific folders. If all folders were then disabled it would be the same as the

blocking component operating globally).

       Examiner recites the same rationale to combine used in claim 2.

26.   **As to Claim 9,** Daniell-Wendkos-Rajan discloses **wherein the system of claim 4, the**

first threshold determined in part by user preferences (Paragraph [0031] of Rajan discloses

additional user-settable configurations may include the ability to name and color-code the spam

directories, as well as the ability to assign their respective ranges. These ranges are seen to be

the same as the thresholds).

       Examiner recites the same rationale to combine used in claim 2.

27.   **As to Claim 18,** Daniell-Wendkos-Rajan discloses **the system of claim 1, further**

comprising a rating component that rates messages as unscanned before they are subjected

to the filtering component (Paragraph [0030] of Rajan discloses as incoming e-mail is received

by the mail server it is graded for spaminess and then moved to the inbox and/or spam

directories. During the time period between reception and being graded it is seen that the letters

are inherently classified as unscanned, since they have no rating and are only moved to the inbox

after being graded).

       Examiner recites the same rationale to combine used in claim 2.

28.   **As to Claim 19,** Daniell-Wendkos-Rajan discloses **the system of claim 18, wherein an**

unscanned message is hidden from view and is not visible in the user's inbox while

additional data about the unscanned message is collected or while the unscanned message is being filtered by the filtering component (Paragraph [0030] of Rajan discloses as incoming e-mail is received by the mail server it is graded for spaminess and then moved to the inbox and/or spam directories. During the time period between reception and being graded it is seen that the letters are inherently classified as unscanned, since they have no rating and are only moved to the inbox after being graded. Since they are not placed into the inbox until after filtering, the messages are effectively hidden from view and are not visible).

Examiner recites the same rationale to combine used in claim 2.

29.   **As to Claim 20,** Daniell-Wendkos-Rajan discloses **the system of claim 18, wherein unscanned messages are made visible in a user's inbox when the filtering component is turned off** (Figure 4 of Daniell discloses being able to turn off spam filtering and next to the selection it is explained that all emails will be delivered to the inbox. Thus it is seen that when filtering is off all messages would be visible).

It is seen that being able to turn off the filter is an obvious feature of the system. Furthermore, once the filter it turned off it is disclosed in Daniell that all emails will be delivered to the inbox. Given that nothing will be marked as spam, none of them would be blocked and as such they would all be visible. Thus it is seen that this limitation is disclosed by Daniell.

30.   **As to Claim 22,** Daniell discloses **a method that mitigates viewing offensive message content comprising:**

employing a processor to execute computer executable instructions stored on a computer

readable medium to perform the following acts (Figure 1 and paragraph [0024] of Daniell

disclose a processor)**;**

receiving at least one message into a memory (Figure 1 and paragraph [0024] of Daniell

disclose the workstations containing an email application that allows the work station to send and

receive email messages through the network)**;**

determining whether content of the at least one message includes text, one or more images,

one or more sounds, one or more videos, one or more URLs, embedded content, one or

more attachments, or one or more applets offensive to the user (Figure 4 of Daniell discloses

a text filtering component that can be used to scan incoming mail for offensive words and

phrases)**; and**

preventing the user from sensing the content of the at least one message determined to be

offensive to the user (Paragraph [0043] of Daniell discloses that, for the spam folder, the feature

of displaying a preview of a selected message has been disabled. This is because the message

has been determined to be objectionable or undesired)

Daniell does not explicitly disclose **computing a junk score for the at least one**

message.

However, Rajan discloses this (Paragraph [0015] of Rajan discloses that each piece of

incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in

paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded

along a 0 - 100 range and this is seen to be a junk score for the messages)**;**

Examiner recites the same rationale to combined used in claim 2.

Daniell does not explicitly disclose **enabling the a user to preview the at least one message in at least a preview pane while** blocking the offensive content.

However, Wendkos discloses this (Paragraph [0008] of Wendkos discloses striping out all images and links from incoming email in an attempt to thwarts computer users from being exposed to offensive images and dangerous links. As seen Wendkos only partially blocks the content of the emails, namely the images and links)

Examiner recites the same rationale to combine used in Claim 1.

Daniell does not explicitly disclose altering the ability to preview **when the junk score exceeds a threshold**

However, Rajan discloses this (Paragraph [0015] of Rajan discloses each piece of mail is graded and then moved into the respective directory according to its level of spaminess. Thus the message no longer appears with the regular mail according to its level of spaminess).

Examiner recites the same rationale to combine used in claim 2.

31.   **As to Claim 24,** Daniell-Wendkos-Rajan discloses **the method of claim 22, further comprising classifying the at least one message as unscanned before computing the junk score** (Paragraph [0030] of Rajan discloses as incoming e-mail is received by the mail server it is graded for spaminess and then moved to the inbox and/or spam directories. During the time period between reception and being graded it is seen that the letters are inherently classified as unscanned, since they have no rating and are only moved to the inbox after being graded).

Examiner recites the same rationale to combine used in claim 2.

32.   **As to Claim 25,** Daniell-Wendkos-Rajan discloses **the method of claim 24, further comprising updating the at least one message from unscanned to some other rating based on, at least in part, its computed junk score** (Paragraph [0030] of Rajan discloses as incoming e-mail is received by the mail server it is graded for spaminess and then moved to the inbox and/or spam directories. During the time period between reception and being graded it is seen that the letters are inherently classified as unscanned, since they have no rating and are only moved to the inbox after being graded. However after being graded it is then moved to the appropriate directories at which point it would be classified under those directories. Thus the score is seen to be updated).

   Examiner recites the same rationale to combine used in claim 2.

33.   **As to Claim 27,** Daniell-Wendkos-Rajan discloses **the method of claim 22, further comprising unblocking blocked content of the at least one message when explicit user input to unblock the blocked message content is received** (Paragraph [0043] of Daniell discloses that messages in the spam folder may be viewed by using the message center to select a message from the spam folder and then selecting the read button. This allows the user to read the text associated with the selected message. Since the message that was in the spam folder was previously not viewable in the preview screen (blocked) and then distinct user input (selecting the read button) allows the letter to be read (unblocked), this is seen to be the same as the claimed limitation).

34.   **As to Claim 34,** Daniell discloses **a system that mitigates viewing offensive message content comprising:**

means for receiving at least one message (Figure 1 and paragraph [0024] of Daniell disclose the workstations containing an email application that allows the work station to send and receive email messages through the network);

means for determining whether content of the at least one message includes text, one or more images, one or more sounds, one or more videos, one or more URLs, embedded content, one or more attachments, or one or more applets associated with information deemed offensive to a user (Figure 4 of Daniell discloses a text filtering component that can be used to scan incoming mail for offensive words and phrases)**; and**

means for blocking the content of the at least one message associated with information deemed offensive to the user from being presented to the user when the at least one message is displayed in at least a preview pane (Paragraph [0015] of Rajan discloses each piece of mail is graded and then moved into the respective directory according to its level of spaminess. Thus the message no longer appears with the regular mail according to its level of spaminess)

wherein instructions associated with one or more of the above means are executed by a processor operatively coupled to memory (Figure 1 and paragraph [0024] of Daniell disclose a processor coupled to memory)**.**

Daniell does not explicitly disclose **means for computing a junk score for the at least one message.**

However, Rajan discloses this(Paragraph [0015] of Rajan discloses that each piece of incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded along a 0 - 100 range and this is seen to be a junk score for the messages);

Examiner recites the same rationale to combine used in claim 2.

Daniell does not explicitly disclose **partially** blocking the content.

However, Wendkos discloses this (Paragraph [0043] of Daniell discloses that, for the spam folder, the feature of displaying a preview of a selected message has been disabled. This is because the message has been determined to be objectionable or undesired. Then paragraph [0008] of Wendkos discloses stripping out all images and links from incoming email. Thus it is seen that Wendkos discloses partially blocking using at least one of the listed limitations);

Examiner recites the same rationale to combine used in claim 1.

Daniell does not explicitly disclose altering the ability to preview **based on the junk score**

However, Rajan discloses this (Paragraph [0015] of Rajan discloses each piece of mail is graded and then moved into the respective directory according to its level of spaminess. Thus the message no longer appears with the regular mail according to its level of spaminess).

Examiner recites the same rationale to combine used in claim 2.

35.   Claims 22 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Daniell and further in view of Rajan.

36.   **As to Claim 22,** Daniell discloses **a method that mitigates viewing offensive message**

content comprising:

employing a processor to execute computer executable instructions stored on a computer

readable medium to perform the following acts (Figure 1 and paragraph [0024] of Daniell

disclose a processor)**;**

receiving at least one message into a memory (Figure 1 and paragraph [0024] of Daniell

disclose the workstations containing an email application that allows the work station to send and

receive email messages through the network);

determining whether content of the at least one message includes text, one or more images,

one or more sounds, one or more videos, one or more URLs, embedded content, one or

more attachments, or one or more applets offensive to the user (Figure 4 of Daniell discloses

a text filtering component that can be used to scan incoming mail for offensive words and

phrases)**; and**

preventing the user from sensing the content of the at least one message determined to be

offensive to the user (Paragraph [0043] of Daniell discloses that, for the spam folder, the feature

of displaying a preview of a selected message has been disabled. This is because the message

has been determined to be objectionable or undesired)

        Daniell does not explicitly disclose **computing a junk score for the at least one**

message.

        However, Rajan discloses this (Paragraph [0015] of Rajan discloses that each piece of

incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in

paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded

along a 0 - 100 range and this is seen to be a junk score for the messages);

Examiner recites the same rationale to combined used in claim 2.

Daniell does not explicitly disclose **<u>enabling the a user to</u> preview the at least one**

message in at least a preview pane <u>while</u> blocking the offensive content.

However, it would have been obvious in view of Daniell's disclosure. Figure 9B of

Daniell discloses allowing a user to make substitutions of objectionable words or phrases. This

is seen to be disclosing partially blocking content by preventing offensive portions of the

message from being viewed. While this is being done manually by a parent for a child it

nonetheless discloses the email client containing a feature used to detect objectionable words for

the purpose of replacing them with acceptable words to prevent only the objectionable content

from being viewed.

It would have been obvious to one of ordinary skill in the art at the time of invention to

combine preventing messages from being viewed in the preview pane as disclosed by Daniell,

with preventing only the objectionable content from being viewed as disclosed by Daniell. One

of ordinary skill in the art would have been motivated to combine to prevent unintentional

viewing of content determined to be objectionable or undesired. Since the purpose of a spam

filtering is to prevent the user from viewing content they do not wish to view, it would be

obvious to prevent the user from seeing the content via the preview pane because the content has

been determined to be objectionable or undesired (Paragraph [0043] of Daniell).

Daniell does not explicitly disclose altering the ability to preview **when the junk score**

exceeds a threshold

However, Rajan discloses this (Paragraph [0015] of Rajan discloses each piece of mail is graded and then moved into the respective directory according to its level of spaminess. Thus the message no longer appears with the regular mail according to its level of spaminess).

Examiner recites the same rationale to combine used in claim 2.

37.   **As to Claim 34,** Daniell discloses **a system that mitigates viewing offensive message content comprising:**

means for receiving at least one message (Figure 1 and paragraph [0024] of Daniell disclose the workstations containing an email application that allows the work station to send and receive email messages through the network)**;**

means for determining whether content of the at least one message includes text, one or more images, one or more sounds, one or more videos, one or more URLs, embedded content, one or more attachments, or one or more applets associated with information deemed offensive to a user (Figure 4 of Daniell discloses a text filtering component that can be used to scan incoming mail for offensive words and phrases)**; and**

means for blocking the content of the at least one message associated with information deemed offensive to the user from being presented to the user when the at least one message is displayed in at least a preview pane (Paragraph [0015] of Rajan discloses each piece of mail is graded and then moved into the respective directory according to its level of spaminess. Thus the message no longer appears with the regular mail according to its level of spaminess)

wherein instructions associated with one or more of the above means are executed by a

processor operatively coupled to memory (Figure 1 and paragraph [0024] of Daniell disclose a

processor coupled to memory).

Daniell does not explicitly disclose **means for computing a junk score for the at least**

one message.

However, Rajan discloses this(Paragraph [0015] of Rajan discloses that each piece of

incoming mail is graded along a scale to determine the level of spaminess of the e-mail. Then in

paragraph [0016] of Rajan an example of the scale shows that incoming mail can be graded

along a 0 - 100 range and this is seen to be a junk score for the messages);

Examiner recites the same rationale to combine used in claim 2.

Daniell does not explicitly disclose **partially** blocking the content.

However, it would have been obvious in view of Daniell's disclosure. Figure 9B of

Daniell discloses allowing a user to make substitutions of objectionable words or phrases. This

is seen to be disclosing partially blocking content by preventing offensive portions of the

message from being viewed. While this is being done manually by a parent for a child it

nonetheless discloses the email client containing a feature used to detect objectionable words for

the purpose of replacing them with acceptable words to prevent only the objectionable content

from being viewed.

It would have been obvious to one of ordinary skill in the art at the time of invention to

combine preventing messages from being viewed in the preview pane as disclosed by Daniell,

with preventing only the objectionable content from being viewed as disclosed by Daniell. One

of ordinary skill in the art would have been motivated to combine to prevent unintentional

viewing of content determined to be objectionable or undesired. Since the purpose of a spam

filtering is to prevent the user from viewing content they do not wish to view, it would be

obvious to prevent the user from seeing the content via the preview pane because the content has

been determined to be objectionable or undesired (Paragraph [0043] of Daniell).

Daniell does not explicitly disclose altering the ability to preview **based on the junk**

score

However, Rajan discloses this (Paragraph [0015] of Rajan discloses each piece of mail is

graded and then moved into the respective directory according to its level of spaminess. Thus

the message no longer appears with the regular mail according to its level of spaminess).

Examiner recites the same rationale to combine used in claim 2.

38.   Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Daniell-Wendkos

and further in view of U.S. Pub. No. 2003/0009495 to Adjaoute (hereinafter "Adjaoute").

39.   **As to Claim 11,** Daniell-Wendkos discloses **the system of claim 1.** Daniell-Wendkos

does not explicitly disclose **wherein the content blocking component replaces blocked**

content of the at least one message with at least one of a text notice, a graphics notice, a

video notice, or an audio notice; and wherein the text notice, graphics notice, video notice

and audio notice warn users that potentially offensive content has been blocked from view.

However, Adjaoute discloses this (Paragraph [0057] of Adjaoute discloses that if the

content is restricted, then a message is displayed instead of the content saying that the access to

the content has been restricted. It is noted that Adjaoute deals primarily with websites however in paragraph [0029] it suggest the software plug-in being installed in an email application).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of claim 1 as disclosed by Daniell-Wendkos, with replacing the blocked content as disclosed by Adjaoute. One of ordinary skill in the art at the time the invention was made would have been motivated to combine in order to help the filter prevent viewing of offensive material. Paragraph [0006] of Adjaoute shares that the goal would be to control the information that children can receive. Thus it is seen that it would be advantageous to block the material and inform the participant that what they are trying to access has been blocked.

40.   Claims 12, 13, 15-17 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Daniell-Wendkos-Rajan and further in view of U.S. Pub. No. 2003/0204569 to Andrews et al. (hereinafter "Andrews").

41.   **As to Claim 12,** Daniell-Wendkos-Rajan discloses **the system of claim 2.** Daniell-Wendkos-Rajan does not explicitly disclose **further comprising a challenge-response component that requests message senders to correctly respond to at least one challenge per message sent by a respective message sender when the junk score of the message sent by the respective message sender exceeds a second threshold, wherein the message sent by the respective message sender is delivered to the user's inbox upon validation of the message sender's response.**

However, Andrews discloses this (Figure 4 of Andrews discloses the process for incoming email messages. As the message flows through the process various things are checked such as whether a message is spam-like, has a potential virus, or if the sender is suspicious. If a message appears to be any of those things the message is issued a challenge. Then in paragraph [0087] of Andrews it is explained that if the system judges that the sender has passed the test the message is placed into the user's inbox).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of claim 1 as disclosed by Daniell-Wendkos-Rajan, with the challenge system disclosed by Andrews. One of ordinary skill in the art at the time the invention was made would have been motivated to combine in order to increase the security of the spam filter. Andrews explains in paragraph [0007] that a challenge would help verify that the source of the potentially infected/spam email is a human and not a machine. Since most spam is generated by a machine as opposed to individually sent out by humans such a system would help filter out many messages.

42.   **As to Claim 13,** Daniell-Wendkos-Rajan-Andrews discloses **the system of claim 12, wherein the second threshold is higher or lower than the first threshold** (Paragraph [0031] of Rajan discloses additional user-settable configurations may include the ability to name and color-code the spam directories, as well as the ability to assign their respective ranges. It is noted that because Rajan discloses a user setting up the configurations for his various spam directories that it would be obvious to either have the second threshold higher or lower depending on the personal preference of the user).

Examiner recites the same rationale to combine used in claim 2.

43.   **As to Claim 15,** Daniell-Wendkos-Rajan-Andrews discloses **the system of claim 12,**

wherein the second threshold is determined at least in part by user preferences (Paragraph

[0031] of Rajan discloses additional user-settable configurations may include the ability to name

and color-code the spam directories, as well as the ability to assign their respective ranges.

These ranges are seen to be the same as the thresholds).

Examiner recites the same rationale to combine used in claim 2.

44.   **As to Claim 16,** Daniell-Wendkos-Rajan-Andrews discloses **the system of claim 12,**

wherein the message sent by the respective message sender is hidden from view in a user's

inbox until the <u>at least one</u> challenge is correctly solved (Figure 1 of Andrews discloses a

letter being detained in the smart email filtering system until a correct response is received. This

is effectively hiding the message from view until it is correctly solved).

Examiner recites the same rationale to combine used in claim 12.

45.   **As to Claim 17,** Daniell-Wendkos-Rajan-Andrews discloses **the system of claim 12,**

wherein content of the message sent by the respective message sender is partially blocked

when the message is released to the user's inbox following a correctly solved challenge

(Figure 4 of Andrews discloses the process for incoming email messages. As the message flows

through the process various things are checked such as whether a message is spam-like, has a

potential virus, or if the sender is suspicious. If a message appears to be any of those things, the

message is issued a challenge. Then in paragraph [0087] of Andrews it is explained that if the

system judges that the sender has passed the test the message is placed into the user's inbox. It is

seen that since the letter was placed into the inbox and that, as disclosed above, letters in the

inbox with sufficient ratings are blocked, it would be obvious that after a message comes back

from a challenge that it would still be blocked once deposited in the inbox).

Examiner recites the same rationale to combine used in claim 12.

46.   **As to Claim 30,** Daniell-Wendkos-Rajan discloses **the method of claim 22.** Daniell-

Wendkos-Rajan does not explicitly disclose **further comprising challenging a sender of the at**

least one message before revealing any blocked content of the at least one message.

However, Andrews discloses this (Figure 4 of Andrews discloses the process for

incoming email messages. As the message flows through the process various things are checked

such as whether a message is spam-like, has a potential virus, or if the sender is suspicious. If a

message appears to be any of those things, the message is issued a challenge. Then in paragraph

[0087] of Andrews it is explained that if the system judges that the sender has passed the test the

message is placed into the user's inbox).

Examiner recites the same rationale to combine used in claim 12.

47.   Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over Daniell-

Wendkos-Rajan and further in view of U.S. Pub. No. 2005/0080889 to Malik et al. (hereinafter

"Malik").

48.   **As to Claim 29,** Daniell-Wendkos-Rajan discloses **the method of claim 22.** Daniell-Wendkos-Rajan does not explicitly disclose **further comprising requiring a password to open messages associated with blocked content.**

However, Malik discloses this (Paragraph [0071] of Malik discloses child protection in an email system where it can be set such that to get access to a child's spam folder one would have to enter in the master or parent password. This is seen to be the same as needing a password to access messages that are blocked)**.**

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of claim 22 as disclosed by Daniell-Wendkos-Rajan, with requiring a password as disclosed by Malik.

One of ordinary skill in the art at the time the invention was made would have been motivated to combine in order to prevent children from viewing content that a parent would deem inappropriate for viewing. Thus it is to provide a method that restricts a child type user from performing a restricted operation (paragraph [0007] Malik).

<div align="center">*Conclusion*</div>

49.   Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this

final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to KEVIN S. MAI whose telephone number is (571)270-5001. The

examiner can normally be reached on Monday through Friday 7:30 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Bunjob Jaroenchonwanit can be reached on 571-272-3913. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/K. S. M./
Examiner, Art Unit 2456

/Yasin M Barqadle/
Primary Examiner, Art Unit 2456